LexisNexis® RISK SOLUTIONS

Customer | IPF Digital

Securing building a better world through financial inclusion for IPF Digital

Industry | Financial Services

Overview

IPF Digital is a leading non-bank lender focused on inclusive finance, serving consumers often overlooked by traditional banks across Europe (including the Baltics and the Czech Republic), Australia and Mexico, while ensuring responsible lending principles and consumer protection laws. To preserve fast, simple onboarding while deterring fraud, IPF Digital uses LexisNexis® ThreatMetrix® as the first fraud gate at application creation. Country-specific policies guide pass/review/reject pathways so trusted customers move quickly, and risky sessions are challenged without blanket friction.

Challenges

- Rising social engineering scams
- Country specific fraud typologies
- Control downstream verification costs
- Minimize friction for customers
- Protect new product launches

"Country-specific policies matter. Fraud in the Baltics, Czech Republic, Australia and Mexico look different; with ThreatMetrix we adapt quickly without adding unnecessary friction or cost."

— Lukas Drvota, IPF Digital Fraud Manager

Our solution

LexisNexis® ThreatMetrix®

ThreatMetrix® is an AI-powered risk decisioning platform that unifies digital identity, device and behavioral intelligence to distinguish trusted users from bad actors in real time. Every IPF Digital application is evaluated against cross-industry intelligence (in compliance with data protection and transfer regulations) from the LexisNexis® Digital Identity Network®, with explainable, policy-driven controls to deliver risk-appropriate experiences, passing low-risk sessions, routing ambiguous cases for review and rejecting high-risk traffic. Placing ThreatMetrix at the first fraud gate reduces downstream costs and keeps onboarding fast for genuine customers.

One platform, many markets: The ThreatMetrix platform runs on a global-intelligence, local-policy model. Common core signals (device, session, network, behavioral) provide consistent context everywhere; country-level policies tailor thresholds and rules to local fraud typologies and regulatory needs; and a continuous feedback loop (reason codes, analyst decisions) enables rapid tuning as patterns evolve. This makes regional differences part of the design, not an exception.

How IPF Digital uses ThreatMetrix

ThreatMetrix is positioned as the first check when an application reaches offer calculation, this ensures risk is assessed before pricing and offer decisions, while avoiding unnecessary friction during earlier lead capture/eligibility steps. Each session receives a digital identity and device risk assessment, leading to: Pass (straight-through), Review (analyst evaluation with reason codes), or Reject (policy-defined high risk). This up-front gate minimizes friction and spend by stepping up only when risk is present, while allowing country-specific rules to emphasize the right signals (e.g., remote-access/coaching indicators for scams; device-sharing/reuse for family fraud; device/IP/geolocation and identity consistency for fake/stolen identities).

> "ThreatMetrix is our first fraud line of defense. Clean applications move quickly; when there are risk signals, we route to review rather than over-rejection. That balance helps us block scams while protecting growth across very different markets."
>
> — Lukas Drvota, IPF Digital Fraud Manager

Business outcomes

How ThreatMetrix has helped with specific regional fraud challenges

Mexico
Up to
95%
reduction in customer care time spent on manual checks for three defined attributes

Czech Republic
Up to
72%
reduction in fraud value after implementing new ThreatMetrix rules using social-engineering flags

Baltics
Approximately
50%
reduction in confirmed scam numbers via early interception and review routing

By positioning ThreatMetrix as the first fraud check, IPF Digital changed the rhythm of onboarding: trusted applicants continued to move through in seconds, while risky sessions were intercepted early, before cost and effort accumulated downstream. This shift meant fewer unnecessary calls to higher-cost services and a more predictable operational load for fraud analysts.

When a wave of social-engineering scams hit the Czech Republic, targeted policy updates (including remote-access and coaching indicators) helped curb losses without blanket friction. Clean traffic still flowed, but questionable applications were diverted for review or declined outright striking a better balance between protection and customer experience, resulting in over 70% fraud value decrease.

The same platform flexed to local realities.

- In the Baltics, refining proprietary risk indicators enabled earlier interception and review routing, helping to reduce confirmed scam numbers by 50%.
- In Mexico, concentration rules targeting personal data reuse shifted work from manual checks to targeted reviews, delivering up to 95% reduction in Customer Care time spent on manual attribute checks, as only ThreatMetrix flagged sessions now require that scrutiny.
- In Australia, device-level intelligence highlighted potential family/first-party patterns so teams could intervene where appropriate, rather than tightening controls for everyone.

Crucially, the operating model positions IPF Digital to support future product enhancements within its regulated framework. As growth initiatives such as Pay Later expand, ThreatMetrix policies can extend to additional touchpoints (including login if credential testing resurges), preserving a low-friction experience for genuine customers while maintaining control of risk and cost.

Let's revolutionize the way you fight fraud

Visit risk.lexisnexis.com/fraudandidentity